

Test your knowledge of pages 460 through 468 in Quiz Yourself 9-1.



QUIZ YOURSELF 9-1

Instructions: Find the true statement below. Then, rewrite the remaining false statements so they are true.

1. A cybercafé is a wireless network that provides Internet connections to mobile computers and other devices.
2. A Web folder is a navigation system that consists of one or more earth-based receivers that accept and analyze signals sent by satellites in order to determine the receiver's geographic location.
3. Web services describe standardized software that enables programmers to create applications that communicate with other remote computers over the Internet or on an internal business network.
4. Receiving devices initiate an instruction to transmit data, instructions, or information.
5. Users can send pictures and sound files, as well as short text messages, with text messaging.

Quiz Yourself Online: To further check your knowledge of required components for communications, sending and receiving devices, and uses of computer communications, visit scsite.com/dc2009/ch9/quiz and then click Objectives 1 – 3.

NETWORKS

As discussed in Chapter 1, a **network** is a collection of computers and devices connected together via communications devices and transmission media. Many businesses network their computers together to facilitate communications, share hardware, share data and information, share software, and transfer funds (Figure 9-9). The next page elaborates on how businesses use networks.

Reasons Businesses Use a Network

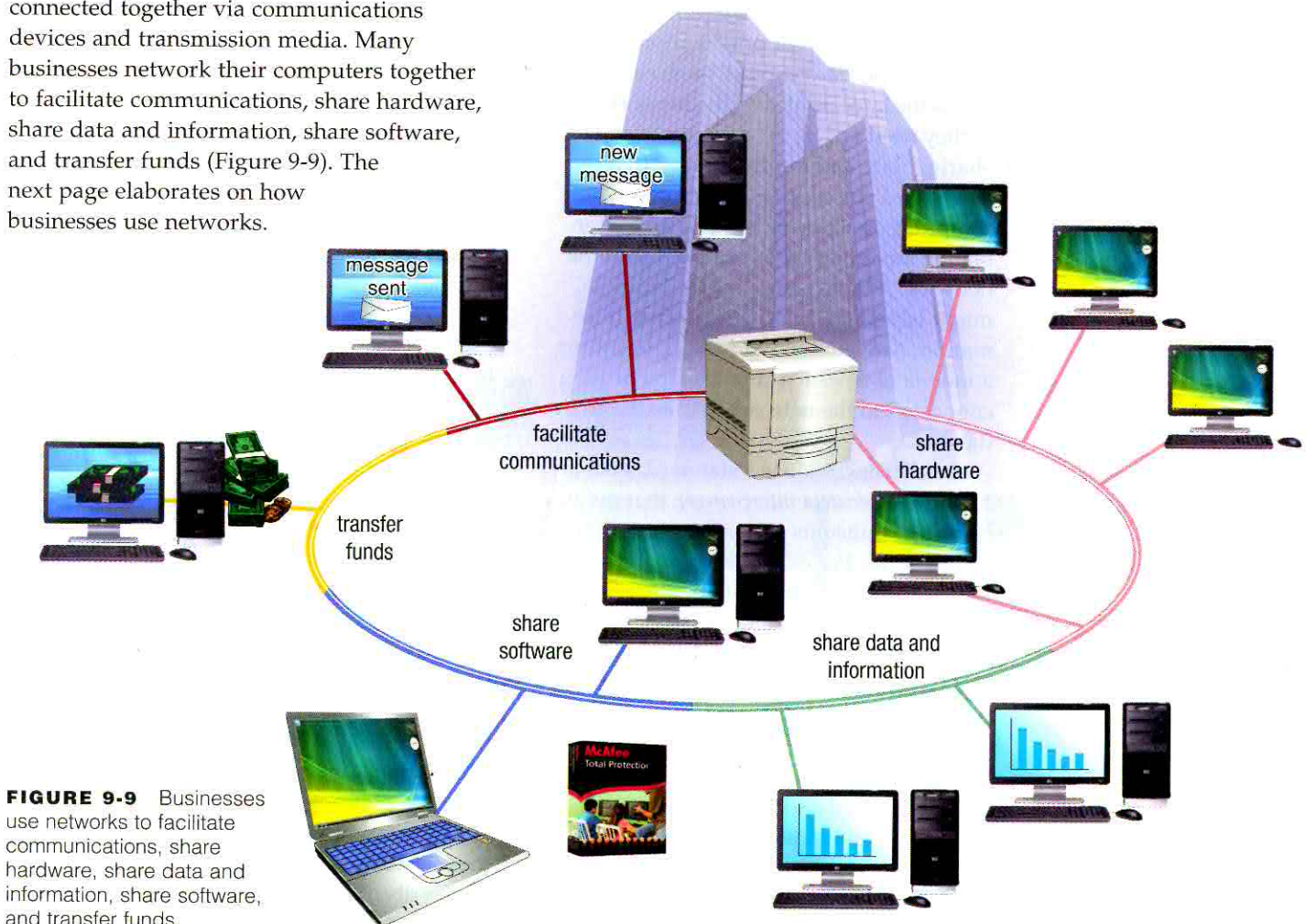


FIGURE 9-9 Businesses use networks to facilitate communications, share hardware, share data and information, share software, and transfer funds.

A network can be internal to an organization or span the world by connecting to the Internet. Networks facilitate communications among users and allow users to share resources, such as data, information, hardware, and software. The following paragraphs explain the advantages of using a network.

- **Facilitating communications** — Using a network, people communicate efficiently and easily via e-mail, instant messaging, chat rooms, blogs, wikis, online social networks, video telephone calls, online meetings, video conferencing, VoIP, wireless messaging services, and groupware. Some of these communications, such as e-mail, occur within a business's internal network. Other times, they occur globally over the Internet.
- **Sharing hardware** — In a networked environment, each computer on the network has access to hardware on the network. Business and home users network their hardware to save money. That is, it may be too costly to provide each user with the same piece of hardware such as a printer. If the computers and a laser printer are connected to a network, the computer users each access the laser printer on the network, as they need it.
- **Sharing data and information** — In a networked environment, any authorized computer user can access data and information stored on other computers on the network. A large company, for example, might have a database of customer information. Any authorized person, including a mobile user with a smart phone or PDA connected to the network, has access to the database.

Most businesses use a standard, such as *EDI (electronic data interchange)*, that defines how data transmits across telephone lines or other means. For example, companies use EDI to handle product catalog distribution, bids, requests for quotations, proposals, order placement, shipping notifications, invoicing, and payment processing. EDI enables businesses to operate with a minimum amount of paperwork.

Another popular data sharing standard is XML, described earlier in this chapter. Using XML, Web programmers can create one version of a Web page that then can be displayed in a form appropriate for a variety of display

devices. XML also is used in RSS, which is used to distribute content, such as news, to subscribers.

- **Sharing software** — Users connected to a network have access to software on the network. To support multiple users' access of software, most vendors sell network versions or site licenses of their software, which usually cost less than buying individual copies of the software for each computer. A *network license* is a legal agreement that allows multiple users to access the software on a server simultaneously. The network license fee usually is based on the number of users or the number of computers attached to the network. A *site license* is a legal agreement that permits users to install the software on multiple computers — usually at a volume discount.
- **Transferring funds** — Called *electronic funds transfer (EFT)*, it allows users connected to a network to transfer money from one bank account to another via transmission media. Both businesses and consumers use EFT. Consumers use an ATM to access their bank account. Businesses deposit payroll checks directly in employees' bank accounts. Consumers use credit cards to make purchases from a retail Web site. Businesses use EFT to purchase and pay for goods purchased from vendors. Both businesses and consumers pay bills online, with which they instruct a bank to use EFT to pay creditors.

Instead of using the Internet or investing in and administering an internal network, some companies hire a value-added network provider for network functions. A *value-added network (VAN)* is a third-party business that provides networking services such as secure data and information transfer, storage, e-mail, and management reports. Some VANs charge an annual or monthly fee; others charge by service used.

For a technical discussion about networks, read the High-Tech Talk article on page 498.

LANs, MANs, and WANs

Networks usually are classified as a local area network, metropolitan area network, or wide area network. The main differentiation among these classifications is their area of coverage, as described in the following paragraphs.

LAN A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as a home, school computer laboratory, office building (Figure 9-10), or closely positioned group of buildings. Each computer or device on the network, called a *node*, often shares resources such as printers, large hard disks, and programs. Often, the nodes are connected via cables.

A **wireless LAN (WLAN)** is a LAN that uses no physical wires. Computers and devices that access a wireless LAN must have built-in wireless capability or the appropriate wireless network card, PC Card, ExpressCard module, USB network adapter, or flash card. Very often, a WLAN communicates with a wired LAN for access to its resources, such as software, hardware, and the Internet (Figure 9-11).

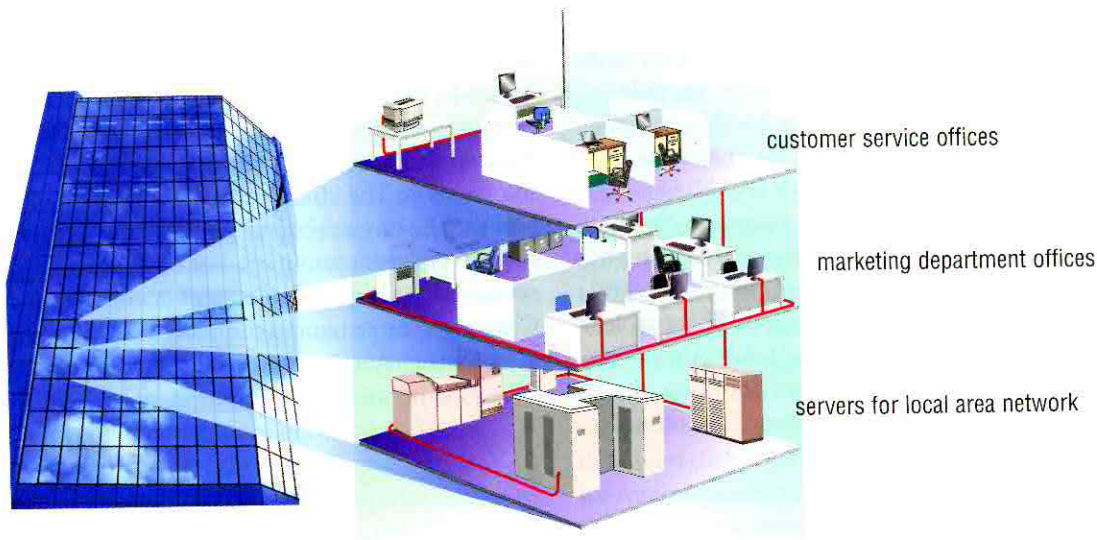


FIGURE 9-10 Computers on different floors access the same local area network (LAN) in an office building.

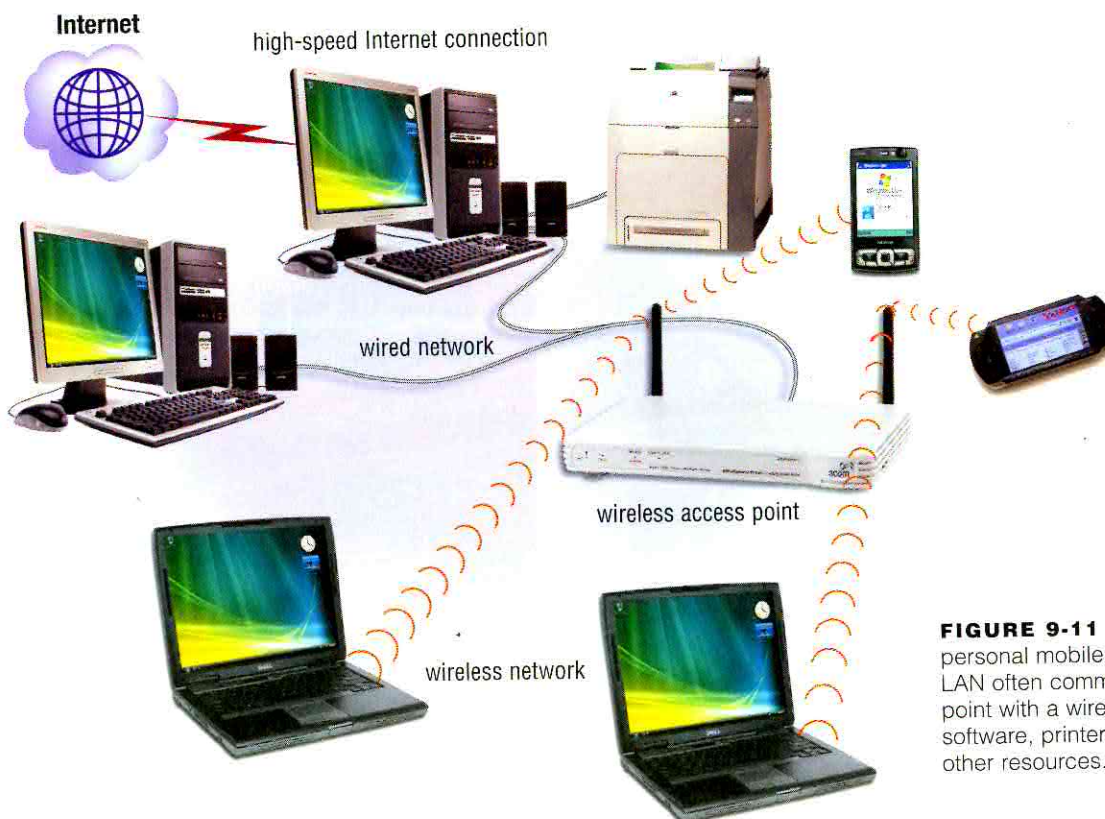


FIGURE 9-11 Computers and personal mobile devices on a wireless LAN often communicate via an access point with a wired LAN to access its software, printer, the Internet, and other resources.

MAN A *metropolitan area network (MAN)* is a high-speed network that connects local area networks in a metropolitan area such as a city or town and handles the bulk of communications activity across that region. A MAN typically includes one or more LANs, but covers a smaller geographic area than a WAN.

A MAN usually is managed by a consortium of users or by a single network provider that sells the service to the users. Local and state governments, for example, regulate some MANs. Telephone companies, cable television operators, and other organizations provide users with connections to the MAN.

WAN A *wide area network (WAN)* is a network that covers a large geographic area (such as a city, country, or the world) using a communications channel that combines many types of media such as telephone lines, cables, and radio waves (Figure 9-12). A WAN can be one large network or can consist of two or more LANs connected together. The Internet is the world's largest WAN.



FIGURE 9-12 An example of a WAN.

Network Architectures

The design of computers, devices, and media in a network, sometimes called the *network architecture*, is categorized as either client/server or peer-to-peer. The following paragraphs discuss these network architectures.

CLIENT/SERVER On a *client/server network*, one or more computers act as a server, and the other computers on the network request services from the server (Figure 9-13). A *server*, sometimes called a *host computer*, controls access to the hardware, software, and other resources on the network and provides a centralized storage area for programs, data, and information. The *clients* are other computers and mobile devices on the network that rely on the server for its resources. For example, a server might store a database of customers. Clients on the network (company employees) access the customer database on the server.

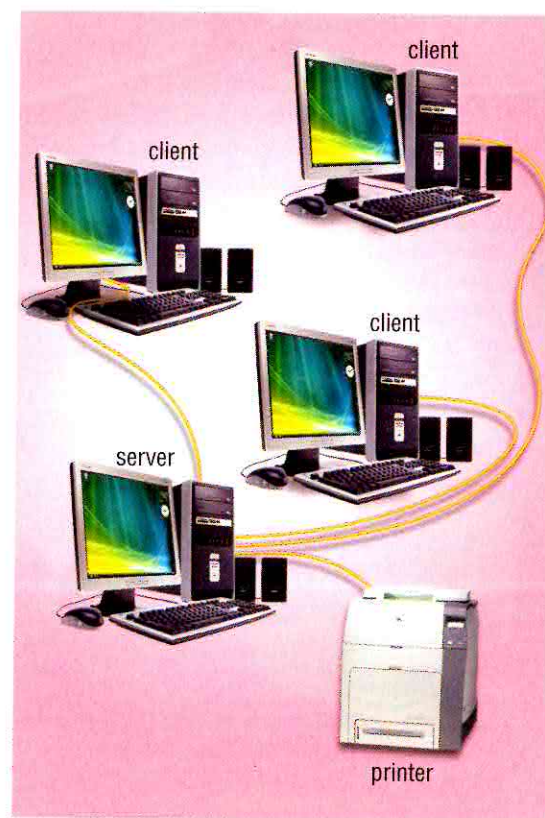


FIGURE 9-13 On a client/server network, one or more computers act as a server, and the clients access the server(s).

Some servers, called *dedicated servers*, perform a specific task and can be placed with other dedicated servers to perform multiple tasks. For example, a *file server* stores and manages files. A *print server* manages printers and documents being printed. A *database server* stores and provides access to a database. A *network server* manages network traffic (activity).

Although it can connect a smaller number of computers, a client/server network typically provides an efficient means to connect 10 or more computers. Most client/server networks require a person to serve as a network administrator because of the large size of the network.

PEER-TO-PEER One type of *peer-to-peer network* is a simple, inexpensive network that typically connects fewer than 10 computers. Each computer, called a *peer*, has equal responsibilities and capabilities, sharing hardware (such as a printer), data, or information with other computers on the peer-to-peer network (Figure 9-14). Each computer stores files on its own storage devices. Thus, each computer on the network contains both the network operating system and application software. All computers

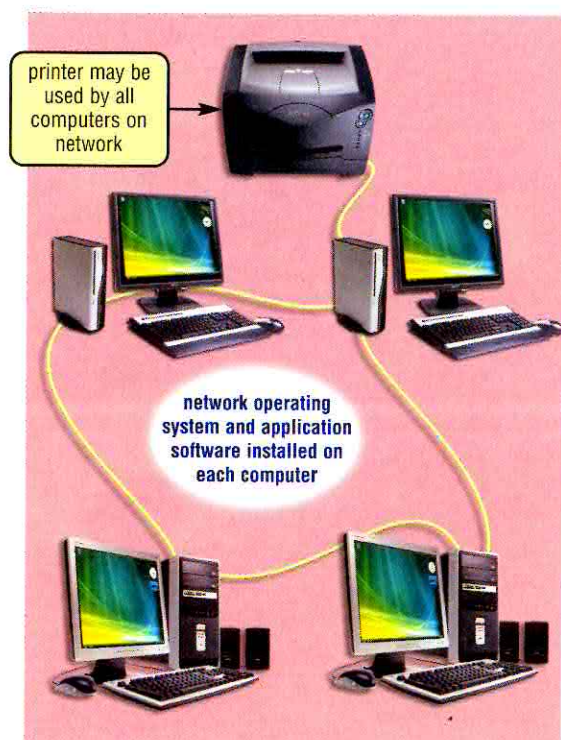


FIGURE 9-14 Each computer on a peer-to-peer network shares its hardware and software with other computers on the network.

on the network share any peripheral device(s) attached to any computer. For example, one computer may have a laser printer and a scanner, while another has an ink-jet printer and an external hard disk.

Peer-to-peer networks are ideal for very small businesses and home users. Some operating systems, such as Windows, include a peer-to-peer networking utility that allows users to set up a peer-to-peer network.

INTERNET PEER-TO-PEER Another type of peer-to-peer, called *P2P*, describes an Internet network on which users access each other's hard disks and exchange files directly over the Internet (Figure 9-15). This type of peer-to-peer network sometimes is called a *file sharing network* because users with compatible software and an Internet connection copy files from someone else's hard disk to their hard disks. As more users connect to the network, each user has access to shared files on other users' hard disks. When users log off the network, others no longer have access to their hard disks. To maintain an acceptable speed for communications, some implementations of P2P limit the number of users.

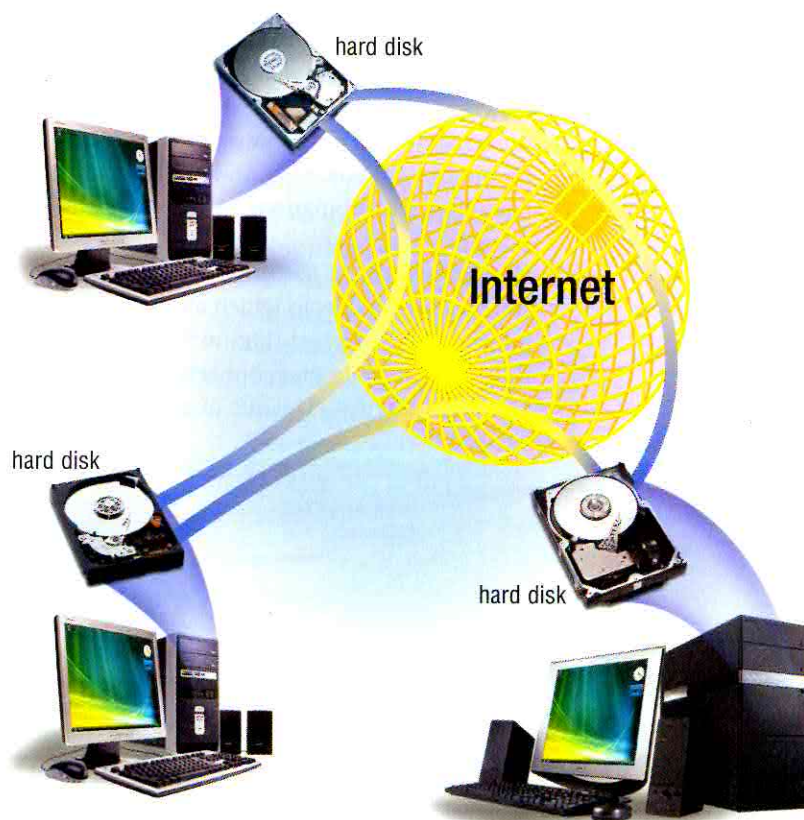


FIGURE 9-15 P2P describes an Internet network on which users connect to each other's hard disks and exchange files directly.



WEB LINK 9-4

BitTorrent

For more information, visit scs.site.com/dc2009/ch9/weblink and then click BitTorrent.

Examples of networking software that support P2P are BitTorrent, Gnutella, Kazaa, and LimeWire, which allow users to swap music and other files via the Web. For example, when one user requests a song, the program searches through lists of shared files — which are stored on one or more connected computers, called supernodes. If a match is found, the music file is copied from the computer on which it resides to the requesting computer. These programs initially stirred much controversy with respect to copyright infringement of music because they allowed users easily to copy music and movie files free from one computer to another. To help reduce copyright infringement, today's music and movie sharing services typically are fee based, and music and movie files often are encrypted as they travel across the Internet.

Many businesses also see an advantage to using P2P. That is, companies and employees can exchange files using P2P, freeing the company from maintaining a network server for this purpose. Business-to-business e-commerce Web sites find that P2P easily allows buyers and sellers to share company information such as product databases.

Network Topologies

A **network topology** refers to the layout of the computers and devices in a communications network. Three commonly used network topologies are bus, ring, and star. Networks usually use combinations of these topologies.

BUS NETWORK A *bus network* consists of a single central cable, to which all computers and other devices connect (Figure 9-16). The *bus* is the physical cable that connects the computers and other devices. The bus in a bus network

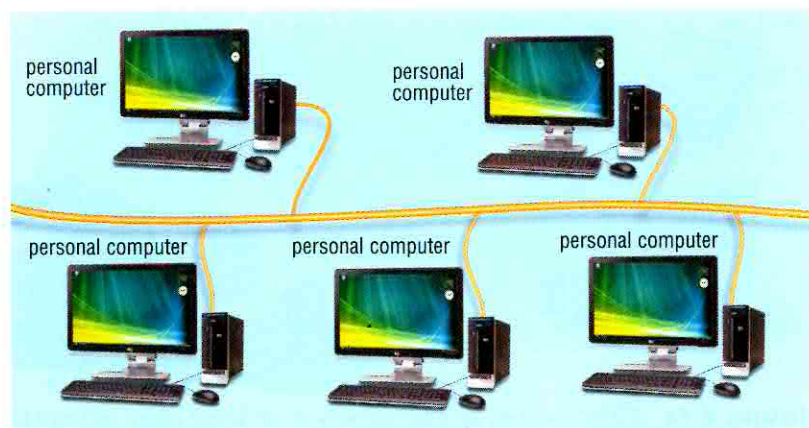


FIGURE 9-16 Devices in a bus network share a single data path.

transmits data, instructions, and information in both directions. When a sending device transmits data, the address of the receiving device is included with the transmission so that the data is routed to the appropriate receiving device.

Bus networks are popular on LANs because they are inexpensive and easy to install. One advantage of the bus network is that computers and other devices can be attached and detached at any point on the bus without disturbing the rest of the network. Another advantage is that failure of one device usually does not affect the rest of the bus network. The greatest risk to a bus network is that the bus itself might become inoperable. If that happens, the network remains inoperative until the bus is back in working order.

RING NETWORK On a *ring network*, a cable forms a closed loop (ring) with all computers and devices arranged along the ring (Figure 9-17). Data transmitted on a ring network travels from device to device around the entire ring, in one direction. When a computer or device sends data, the data travels to each computer on the ring until it reaches its destination.

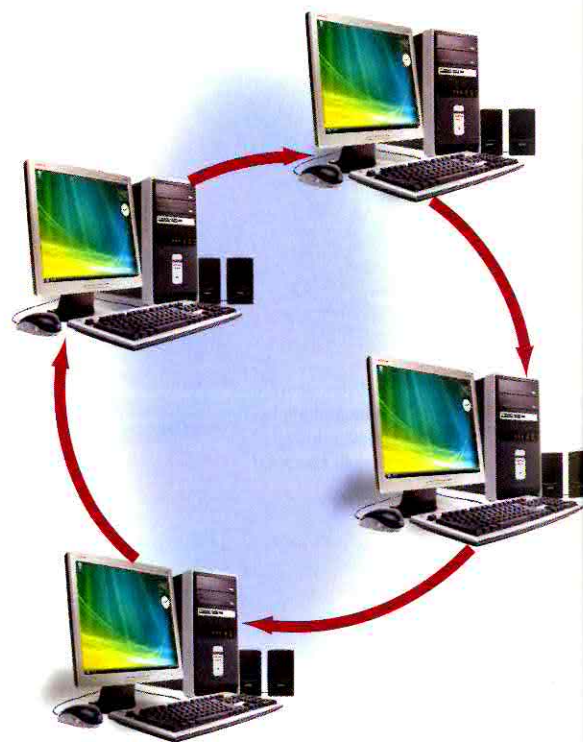


FIGURE 9-17 On a ring network, all connected devices form a continuous loop.

If a computer or device on a ring network fails, all devices before the failed device are unaffected, but those after the failed device cannot function. A ring network can span a larger distance than a bus network, but it is more difficult to install. The ring topology primarily is used for LANs, but also is used in WANs.

STAR NETWORK On a *star network*, all of the computers and devices (nodes) on the network connect to a central device, thus forming a star (Figure 9-18). Two types of devices that provide a common central connection point for nodes on the network are a *hub* and a *switch*. All data that transfers from one node to another passes through the hub/switch.

Star networks are fairly easy to install and maintain. Nodes can be added to and removed from the network with little or no disruption to the network.

On a star network, if one node fails, only that node is affected. The other nodes continue to operate normally. If the hub/switch fails, however, the entire network is inoperable until the device is repaired. Most large star networks, therefore, keep backup hubs/switches available in case the primary one fails.

Intranets

Recognizing the efficiency and power of the Internet, many organizations apply Internet and Web technologies to their own internal networks. An *intranet* (intra means within) is an internal network that uses Internet technologies. Intranets generally make company information accessible to employees and facilitate working in groups.

Simple intranet applications include electronic publishing of organizational materials such as telephone directories, event calendars, procedure manuals, employee benefits information, and job postings. Additionally, an intranet typically includes a connection to the Internet. More sophisticated uses of intranets include groupware applications such as project management, chat rooms, newsgroups, group scheduling, and video conferencing.

An intranet essentially is a small version of the Internet that exists within an organization. It has a Web server, supports multimedia Web pages coded in HTML, and is accessible via a Web browser such as Internet Explorer, Firefox, Opera, and Safari. Users update information on the intranet by creating and posting a Web page, using a method similar to that used on the Internet.

Sometimes a company uses an *extranet*, which allows customers or suppliers to access part of its intranet. Package shipping companies, for example, allow customers to access their intranet to print air bills, schedule pickups, and even track shipped packages as the packages travel to their destinations.

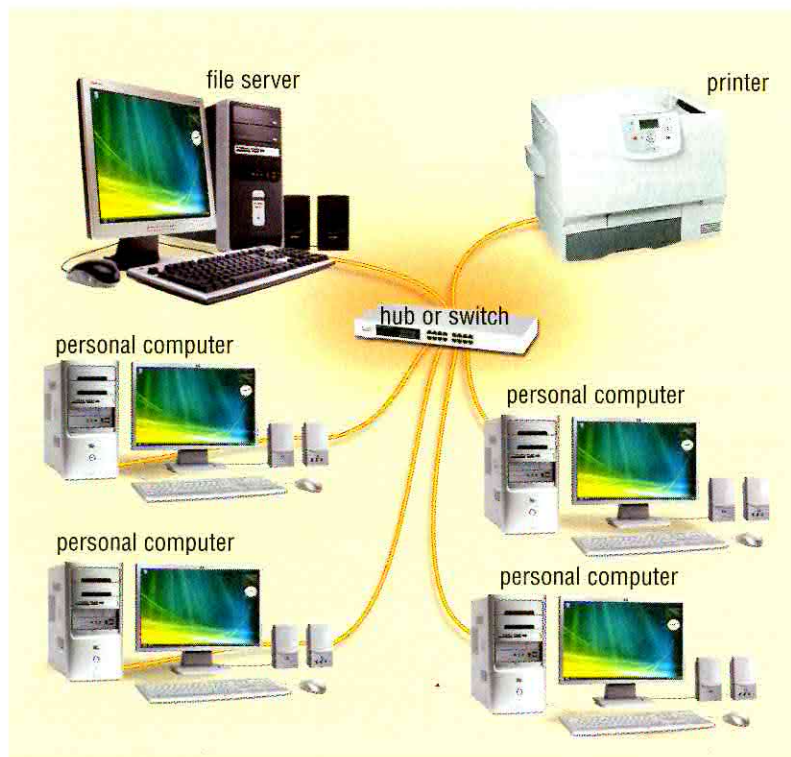


FIGURE 9-18 A star network contains a single, centralized hub or switch through which all the devices in the network communicate.

NETWORK COMMUNICATIONS STANDARDS

Today's networks connect terminals, devices, and computers from many different manufacturers across many types of networks, such as wide area, local area, and wireless. For the different devices on various types of networks to be able to communicate, the network must use similar techniques of moving data through the network from one application to another. For example, an IBM mainframe computer cannot communicate directly with an Apple Macintosh network — some form of translation must occur for devices on these two types of networks to communicate.

To alleviate the problems of incompatibility and ensure that hardware and software components can be integrated into any network, various organizations such as ANSI and IEEE (pronounced I triple E) propose, develop, and approve network standards. A *network standard* defines guidelines that specify the way computers access the medium to which they are attached, the type(s) of medium used, the speeds used on different types of networks, and the type(s) of physical cable and/or the wireless technology used. A standard that outlines characteristics of how two network devices communicate is called a *protocol*. Specifically, a protocol may define data format, coding schemes, error handling, and sequencing techniques. Hardware and software manufacturers design their products to meet the guidelines specified in a particular standard, so that their devices can communicate with the network.

The following sections discuss some of the more widely used network communications standards and protocols for both wired and wireless networks including Ethernet, token ring, TCP/IP, 802.11 (Wi-Fi), Bluetooth, UWB, IrDA, RFID, WiMAX, and WAP. Oftentimes, these network standards and protocols work together to move data through a network. Some of these standards define how a network is arranged physically; others specify how messages travel along the network, and so on. Thus, as data moves through the network from one program to another, it may use one or more of these standards.

Ethernet

Ethernet is a network standard that specifies no central computer or device on the network (nodes) should control when data can be transmitted; that is, each node attempts to transmit data when it determines the network is available to receive communications. If two computers on an Ethernet network attempt to send data at the same time, a collision will occur, and the computers must attempt to send their messages again.

Ethernet is based on a bus topology, but Ethernet networks can be wired in a star pattern. The Ethernet standard defines guidelines for the physical configuration of a network, e.g., cabling, network cards, and nodes. Today, Ethernet is the most popular network standard for LANs because it is relatively inexpensive and easy to install and maintain.

Ethernet networks often use cables to transmit data. At a 10 Mbps (million bits per second) data transfer rate, the original Ethernet standard is not very fast by today's standards. A more recent Ethernet standard, called *Fast Ethernet*, has a data transfer rate of 100 Mbps, ten times faster than the original standard. *Gigabit Ethernet* provides an even higher speed of transmission, with transfer rates of 1 Gbps (1 billion bits per second). The *10-Gigabit Ethernet* standard supports transfer rates up to 10 Gbps.

Token Ring

The **token ring** standard specifies that computers and devices on the network share or pass a special signal, called a token, in a unidirectional manner and in a preset order. A *token* is a special series of bits that function like a ticket. The device with the token can transmit data over the network. Only one token exists per network. This ensures that only one computer transmits data at a time.

Token ring is based on a ring topology (although it can use a star topology). The token ring standard defines guidelines for the physical configuration of a network, e.g., cabling, network cards, and devices. Some token ring networks connect up to 72 devices. Others use a special type of wiring that allows up to 260 connections. The data transfer rate on a token ring network can be 4 Mbps, 16 Mbps, 100 Mbps, or 1 Gbps.



WEB LINK 9-5

Ethernet

For more information, visit scs.site.com/dc2009/ch9/weblink and then click Ethernet.

TCP/IP

Short for *Transmission Control Protocol/Internet Protocol*, **TCP/IP** is a network standard, specifically a protocol, that defines how messages (data) are routed from one end of a network to the other, ensuring the data arrives correctly. TCP/IP describes rules for dividing messages into small pieces, called *packets*; providing addresses for each packet; checking for and detecting errors; sequencing packets; and regulating the flow of messages along the network.

TCP/IP has been adopted as a network standard for Internet communications. Thus, all hosts on the Internet follow the rules defined in this standard. As shown in Figure 9-19, Internet communications also use other standards, such as the Ethernet standard, as data is routed to its destination.

When a computer sends data over the Internet, the data is divided into packets. Each packet contains the data, as well as the recipient

(destination), the origin (sender), and the sequence information used to reassemble the data at the destination. Each packet travels along the fastest individual available path to the recipient's computer via communications devices called routers.

This technique of breaking a message into individual packets, sending the packets along the best route available, and then reassembling the data is called *packet switching*.

FAQ 9-1

Do HTTP, SMTP, and POP work with TCP/IP?

Yes. HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), and POP (Post Office Protocol) are standards that define the format of data as it transmits over networks that use the TCP/IP standard. HTTP works with Web browsers, and SMTP and POP work with e-mail programs. For more information, visit scs.site.com/dc2009/ch9/faq and then click HTTP, SMTP, and POP.

EXAMPLE OF HOW COMMUNICATIONS STANDARDS WORK TOGETHER

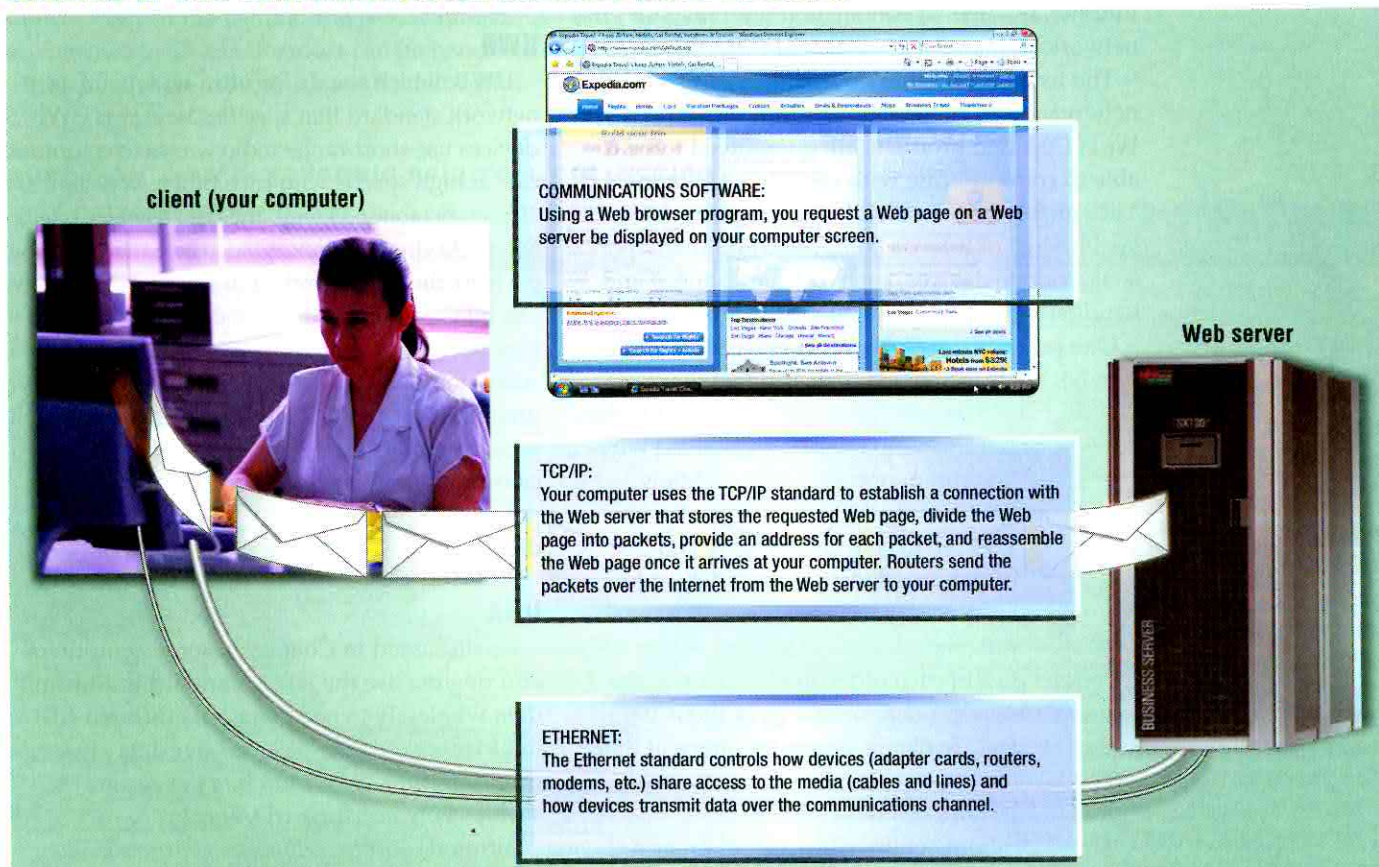


FIGURE 9-19 Network communications use a variety of standards to ensure that data travels correctly to its destination. Some standards used in Internet communications include the TCP/IP and Ethernet standards, as shown in this figure.

802.11 (Wi-Fi)

Developed by IEEE, **802.11** is a series of network standards that specifies how two wireless devices communicate over the air with each other. Using the 802.11 standard, computers or devices that have the appropriate wireless capability communicate via radio waves with other computers or devices. The table in Figure 9-20 outlines various 802.11 standards and their data transfer rates. A

802.11 SERIES OF STANDARDS

Standard	Transfer Rates
802.11	1 or 2 Mbps
802.11a	Up to 54 Mbps
802.11b	Up to 11 Mbps
802.11g	54 Mbps and higher
802.11n	108 Mbps and higher

FIGURE 9-20

A comparison of standards in the 802.11 series.

designation of 802.11 a/b/g on a computer or device indicates it supports all three standards. The newest standard, 802.11n, uses multiple transmitters and receivers, known as *MIMO* (multiple-input multiple-output), to reach speeds from 2 to 10 times faster than 802.11g.

The 802.11 standard often is called the *wireless Ethernet standard* because it uses techniques similar to the

Ethernet standard to specify how physically to configure a wireless network. Thus, 802.11 networks easily can be integrated with wired Ethernet networks. When an 802.11 network accesses the Internet, it works in conjunction with the TCP/IP network standard.

The term **Wi-Fi** (*wireless fidelity*) identifies any network based on the 802.11 series of standards. Wi-Fi Certified products are guaranteed to be able to communicate with each other. Windows Vista and Windows Mobile include support for Wi-Fi. Most of today's computers and many personal mobile devices, such as smart phones and handheld game consoles, are Wi-Fi enabled.

One popular use of the Wi-Fi network standard is in hot spots (discussed earlier in this chapter) that offer mobile users the ability to connect to the

Internet with their Wi-Fi enabled wireless computers and devices. Many homes and small businesses also use Wi-Fi to network computers and devices wirelessly. In open or outdoor areas free from interference, the computers or devices should be within 300 feet of each other. In closed areas, the wireless network range is about 100 feet. To obtain communications at the maximum distances, you may need to install extra hardware.

Some entire cities are set up as a *Wi-Fi mesh network*, in which each mesh node routes its data to the next available node until the data reaches its destination — usually an Internet connection. A Wi-Fi mesh network is

more flexible than a hot spot because each node in a mesh network does not have to be directly connected to the Internet.

Bluetooth

Bluetooth is a network standard, specifically a protocol, that defines how two Bluetooth devices use short-range radio waves to transmit data. The data transfers between devices at a rate of up to 3 Mbps. To communicate with each other, Bluetooth devices often must be within about 10 meters (about 33 feet) but can be extended to 100 meters with additional equipment.

A Bluetooth device contains a small chip that allows it to communicate with other Bluetooth devices. Examples of Bluetooth-enabled devices can include desktop computers, notebook computers, handheld computers, smart phones, PDAs, headsets, keyboards, mouse devices, microphones, digital cameras, and printers. For computers and devices not Bluetooth-enabled, you can purchase a Bluetooth wireless port adapter that will convert an existing USB port or serial port into a Bluetooth port. Windows Vista has built-in Bluetooth support.

UWB

UWB, which stands for **ultra-wideband**, is a network standard that specifies how two UWB devices use short-range radio waves to communicate at high speeds with each other. At distances of 10 meters (about 33 feet), the data transfer rate is 110 Mbps. At closer distances, such as 2 meters (about 6.5 feet), the transfer rate is at least 480 Mbps. UWB can transmit signals through doors and other obstacles. Because of its high transfer rates, UWB is best suited for transmission of large files such as video, graphics, and audio. Examples of UWB uses include wirelessly transferring video from a digital video camera, printing pictures from a digital camera, downloading media to a portable media player, or displaying a slide show on a projector.

IrDA

As discussed in Chapter 4, some computers and devices use the **IrDA** standard to transmit data wirelessly to each other via infrared (IR) light waves. The devices transfer data at rates from 115 Kbps (thousand bits per second) to 4 Mbps between their IrDA ports.

Infrared requires a *line-of-sight transmission*; that is, the sending device and the receiving device must be in line with each other so that nothing obstructs the path of the infrared light wave. Because Bluetooth and UWB do not require line-of-sight transmission, some industry experts



FAQ 9-2

How do I know where hot spots exist?

If your computer has wireless capability that is enabled, Windows automatically will search for hot spots. If a hot spot exists, Windows will display an indication in the notification area on the taskbar. New notebook computers also may have a switch that allows you to determine if a hot spot exists, without turning on the computer. For more information, visit scs.site.com/dc2009/ch9/faq and then click Hot Spots.

predict that these technologies will replace infrared.

RFID

RFID (*radio frequency identification*) is a standard, specifically a protocol, that defines how a network uses radio signals to communicate with a tag placed in or attached to an object, an animal, or a person. The tag, called a transponder, consists of an antenna and a memory chip that contains the information to be transmitted via radio waves. Through an antenna, an RFID reader, also called a transceiver, reads the radio signals and transfers the information to a computer or computing device.

RFID tags are passive or active. An active RFID tag contains a battery that runs the chip's circuitry and broadcasts a signal to the RFID reader. A passive RFID tag does not contain a battery and thus cannot send a signal until the reader activates the tag's antenna by sending out electromagnetic waves. Because passive RFID tags contain no battery, these can be small enough to be embedded in skin.

Depending on the type of RFID reader, the distance between the tag and the reader ranges from 5 inches to 15 feet. Readers can be handheld or embedded in an object such as the tollbooth shown in Figure 9-21.

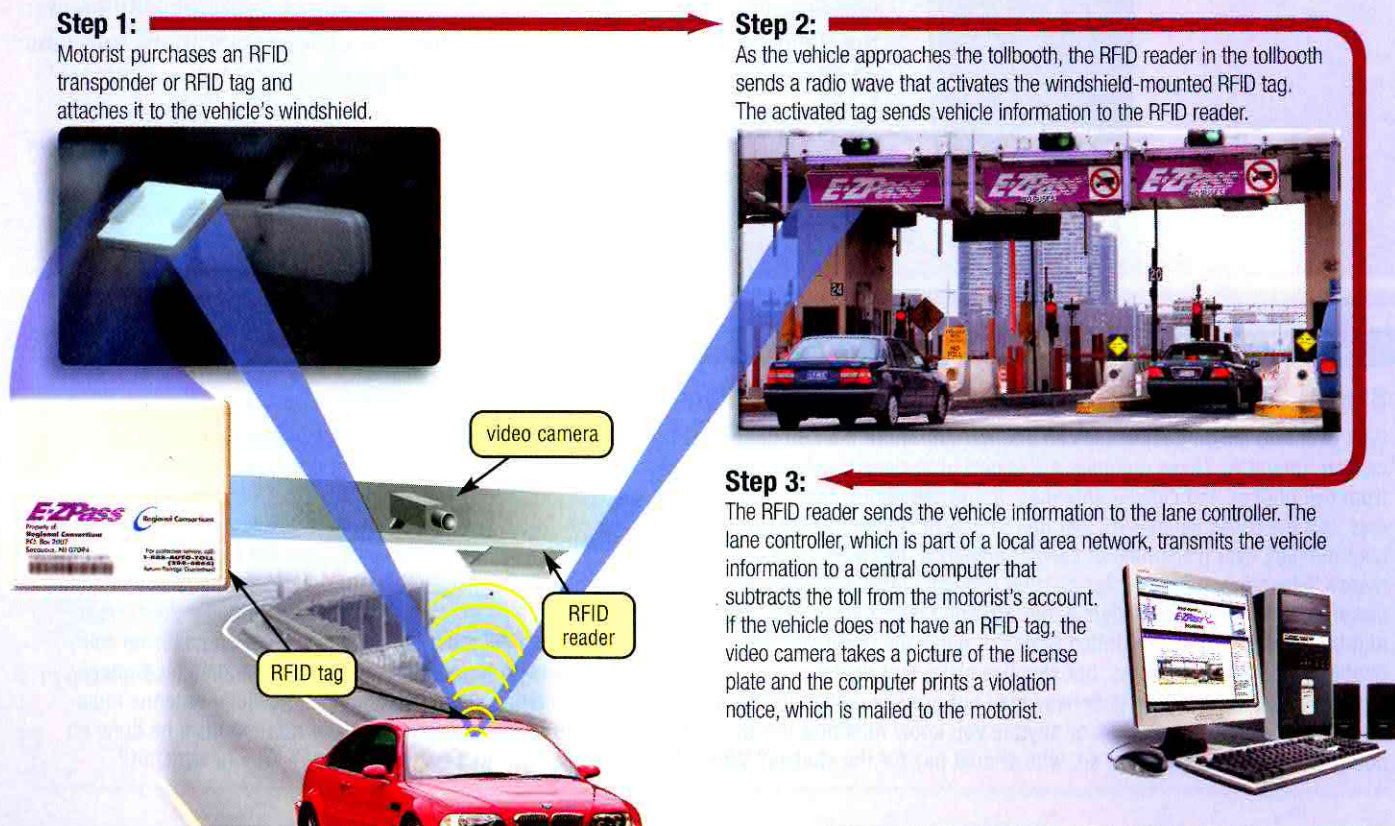
WiMAX

WiMAX (Worldwide Interoperability for Microwave Access), also known as **802.16**, is a newer network standard developed by IEEE that specifies how wireless devices communicate over the air in a wide area. Using the WiMAX standard, computers or devices with the appropriate WiMAX wireless capability communicate via radio waves with other computers or devices via a WiMAX tower. The WiMAX tower, which can cover up to a 30-mile radius, connects to the Internet or to another WiMAX tower.

The WiMAX Forum is a wireless industry association of more than 480 suppliers and Internet access providers dedicated to developing specifications and testing equipment. Two types of WiMAX specifications defined by the WiMAX forum are fixed wireless and mobile wireless. With fixed wireless WiMAX, a customer accesses the Internet from a desktop computer at home or other permanent location. Mobile wireless WiMAX, by contrast, enables users to access the WiMAX network with mobile computers and mobile devices such as smart phones. Fixed wireless WiMAX has data transfer rates up to 40 Mbps, while mobile wireless WiMAX has data transfer rates up to 15 Mbps.

The WiMAX standard provides wireless broadband Internet access at a reasonable cost

FIGURE 9-21 HOW ELECTRONIC RFID TOLL COLLECTION WORKS





WEB LINK 9-6

WIMAX

For more information, visit scs.site.com/dc2009/ch9/weblink and then click WiMAX.

over long distances to business and home users. Experts predict that WiMAX service eventually could surpass other broadband Internet access services such as DSL and cable because it can reach rural and remote areas easily and inexpensively. The WiMAX standard, similar to the Wi-Fi standard, connects mobile users to the Internet via hot spots. Many computers and mobile devices such as smart phones have built-in WiMAX capability. The next generation of game consoles also plans to support the WiMAX standard.

WAP

The **Wireless Application Protocol (WAP)** is a standard, specifically a protocol, that specifies how some mobile devices such as smart phones can display the content of Internet services such as the Web, e-mail, and chat rooms. For example, users can check weather, sports scores, and headline news from their WAP-enabled smart

phone. To display a Web page on a smart phone, the phone should contain a microbrowser (Figure 9-22). WAP works in conjunction with the TCP/IP network standard.

WAP uses a client/server network. The wireless device contains the client software, which connects to the Internet access provider's server. On WAP-enabled devices, data transfer rates range from 9.6 to 153 Kbps

depending on the type of service. Read Ethics & Issues 9-3 for a discussion related to wireless mobile devices.

COMMUNICATIONS SOFTWARE

Communications software consists of programs that (1) help users establish a connection to another computer or network; (2) manage the transmission of data, instructions, and information; and (3) provide an interface for users to communicate with one another. The first two are system software and the third is application software. Chapter 3 presented a variety of examples of application software for communications: e-mail, FTP, Web browser, newsgroup/message boards, chat rooms, instant messaging, video conferencing, and VoIP.

Sometimes, communications devices are pre-programmed to accomplish communications tasks. Other communications devices require separate communications software to ensure proper transmission of data. Communications software works with the network standards and protocols just discussed to ensure data moves through the network or the Internet correctly. Communications software usually is bundled with the operating system or purchased network devices.

Often, a computer has various types of communications software, each serving a different purpose. One type of communications software, for example, helps users establish an Internet connection using wizards, dialog boxes, and other on-screen messages. Another allows home and small office users to configure wired and wireless networks and connect devices to an existing network.



FIGURE 9-22
A WAP-enabled smart phone.

ETHICS & ISSUES 9-3

Should You Worry about Cell Phone and Cellular Antenna Radiation?

Well over two billion people use cell phones, and more than 80 percent of the world's population has access to cell phone service from cellular antennas. These numbers are expected to rise sharply in coming years, and many are concerned about potential health effects from cell phones and cellular antennas. Some cell phone users who suffered rare illnesses have filed lawsuits against cell phone companies, but the cases usually are lost due to lack of scientific evidence linking the use of the phones to the illnesses. While debates rage in communities over placement of cellular antennas, the consideration of health effects on residents is muted because the federal government's Telecommunications Act of 1996 prohibits local governments from considering health effects when making decisions about antenna placement. As cellular providers begin offering faster Internet services, they estimate that they may need to more than double the current number of antennas in the United States. It generally is agreed that no studies conclusively demonstrate negative health effects from cell phones and cellular antennas, but skeptics claim that digital cellular technology is too new to have endured long-term studies on humans. Long-term studies that are underway may not provide results for decades. Are you concerned about cell phone and cellular antenna radiation? Why or why not? Do you or anyone you know minimize use of cell phones due to health concerns? Should more studies be done on potential health effects, and if so, who should pay for the studies? Why? Would you live next to a cellular antenna? Why or why not?